UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

UNITED STATES OF AMERICA)
)
v.) Case No. 2:16-cr-73
)
CHRISTOPHER JOSEPH SCANLON)

OPINION AND ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE AND STATEMENTS
(Doc. 21)

This matter came before the court for a hearing on November 30, 2016 and February 16, 2017 on Defendant Christopher Joseph Scanlon's motion to suppress evidence and statements. (Doc. 21.) On January 27, 2017, the parties submitted a stipulation of facts (Doc. 27) which the court adopted. The court also received into evidence, without objection, government's exhibit 1, which is a transcript and exhibits from a June 23, 2016 motion hearing held in the Western District of Arkansas in *United States v. Anthony Allen Jean*, Case No. 5:15-cr-50087-001 and government's exhibit 2, which is a transcript and exhibits from a January 22, 2016 motion hearing in the Western District of Washington in *United States v. Jay Michaud,* Case No. 15-cr-5351RBJ.

Defendant filed a post-hearing memorandum on February 27, 2017, at which time the court took his motion to suppress under advisement. (Doc. 29.)

Defendant is charged in a one-count Indictment with knowingly accessing with the intent to view child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). He seeks suppression of all evidence derived from the search of his computer and residence and any inculpatory statements he made to law enforcement officers. He argues that Magistrate Judge Theresa C. Buchanan of the Eastern District of Virginia lacked jurisdiction to issue a search warrant for his property and that no exception to Fed. R. Crim. P. 41 applies. The government opposes the motion, arguing that the warrant was validly issued under Fed. R. Crim. P. 41(b) or, in the alternative, that the good faith exception to the exclusionary rule applies rendering suppression inappropriate.

The government is represented by Assistant United States Attorney Jonathan Ophardt. Defendant is represented by Federal Public Defender Michael L. Desautels and Assistant Federal Public Defendant Barclay T. Johnson.

I. Findings of Fact.

Defendant is alleged to have been identified by his Internet Protocol ("IP") address as a visitor to the Playpen website located on the Onion Router ("Tor") network. An IP address is "a unique number used by a computer to access the Internet." (Doc. 21-2 at 11.) An IP address is "dynamic" if a user's internet service provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet. *Id.* An IP address is "static" if a user's ISP assigns a particular IP address to the user's computer which is used each time the computer accesses the Internet. *Id.* IP addresses are also used by computer servers, including web servers, to communicate with other computers.

The Tor network was originally designed and implemented as a project of the United States Naval Research Laboratory for the primary purpose of protecting governmental communications. It is now available to the public although it continues to receive support and funding from the federal government. The Tor network is designed to protect the anonymity of its users by employing a series of computers to prevent disclosure of the IP addresses of computers that access it. The Tor network can be used for both legal and illegal purposes.

Websites outside the Tor network generally maintain IP address logs that can be used to locate and identify a website's users. Law enforcement can use investigative methods to gain access to those logs and to perform a publicly available search to determine the ISP associated with a target IP address. Law enforcement may then subpoena the ISP for records that will enable it determine the identity of the user to whom an IP address was assigned at a specified date and time.

Because of the way Tor routes user communications, traditional IP identification techniques are not viable. For example, when a Tor network user accesses a website, the

IP address of a Tor "exit node," the last computer through which the user's communication was routed, appears in the website's IP log as opposed to the user's actual IP address. As a result, the IP address logs of a Tor-based website cannot be used to locate and identify administrators and users.

The Tor network includes certain websites known as "hidden services." A hidden service operates similarly to a traditional website except that the IP address for a hidden service's web server is concealed and replaced with a Tor-based algorithm ending in ".onion." In order to access a hidden service, a user must use special Tor software and the Tor network. Unlike a traditional website, law enforcement cannot use Tor-generated IP addresses and publicly available searches to identify the location of a hidden service host computer. Tor's search engine does not list hidden services located on the Tor network and actively bans child pornography websites from its search results.

During its operation, Playpen was a hidden service on the Tor network. In order to access it, a user had to download the Tor browser which is available from the Tor project website and install Tor software on his or her computer either by downloading an add-on to the user's web browser or by downloading the Tor browser bundle. A user could not simply perform a Google search to locate the Playpen website, but would instead need to find a link to it either on index sites that provide links to child pornography websites or by communicating with other users. In light of Playpen's status as a hidden service, in the opinion of FBI Special Agent Daniel Alfin: "It would be incredibly unlikely for someone to accidentally stumble on the Playpen website without knowing what its purpose was." Gov't Ex. 1, p. 20, lines 14-16.

After clicking on the link to the Playpen website, a user was presented with a homepage which depicts what appear to be two prepubescent females on either side of the Playpen logo: one wearing a short sleeve shirt and what appears to be underwear and the other wearing a bikini type costume. Both females are positioned with their legs spread so that their clothed crotch areas are visible. Underneath their images is the following statement: "No cross-board reports, .7z preferred, encrypt filenames, include preview. Peace out." *Id.* at 22, lines 18-24 (internal quotation marks omitted).

According to Special Agent Alfin, "these terms [are] a trade craft associated with child pornography websites. These terms and variations of them appear on multiple child pornography websites." *Id.* at 23, lines 1-4. He provided the following translation:

> [N]o cross-board reposts is a warning indicating that a user of Playpen should not go to another child porn website, find a link to an image or a video of child porn and then come back to Playpen and post that link there and claim credit for it themselves.
>
> ".7z preferred" indicate users who share child pornography on the Playpen website should use 7-Zip . . . compression software to share their material. 7-Zip is, again, certainly not illegal. It's freely available software that can be used to compress files, multiple files, into a smaller one. It also adds security benefits. Material provided in a 7-Zip encrypted file can be encrypted with fairly strong encryption that can be difficult or impossible to break, which is why it is the preferred method of distributing child pornography.
>
> "Encrypt filenames" is another reference to an option within the 7-Zip software and so if you have placed child pornography inside one of these 7-Zip archives, you encrypt both the material and the filenames of the material inside of it and so an outside observer who obtained that file, if they don't have the true password, they would have no idea what is contained in that file. It could be innocent material; it could be illegal material. They would have no way of knowing.
>
> "Include preview" is a reference to how users should post material on the website. Generally material that was distributed on Playpen and other such websites is done through an encrypted archives as described previously. However, users are encouraged to post a preview of the material that they are sharing. So generally if a user were to post[]. . . a 30-minute video, a user would post a link to the 7-Zip file that contains that video, and they would also post some screen captures from the video so a user could see what the video depicts before deciding whether or not they want to download the entire video. And so all of those lines up there, aside from "peace out" are, based on my training and experience, trade craft common to child pornography sites.

Id. at 23-24.

After a user arrives at the homepage of the Playpen website, a user must do one of two things to proceed further. If a user has previously accessed the contents of the Playpen website, he or she must enter a previously created username and password and log into the Playpen website using that established account. If a user has not visited the

Playpen website previously or wants to create a new account, he or she would have to click on the "register a new account" link which would take the user to another webpage.

In registering an account, the Playpen website cautions users not to enter a real e-mail address and provides the following instructions and guidance:

> VERY IMPORTANT. READ ALL OF THIS PLEASE.
>
> I will add to this as needed.
>
> The software that we use for this forum requires that new users enter an email address, and checks that what you enter looks approximately valid. We can't turn this off but the forum operators do NOT want you to enter a real address, just something that matches the xxx@yyy.zzz pattern. No confirmation email will be sent. This board has been intentionally configured so that it WILL NOT SEND EMAIL, EVER. Do not forget your password, you won't be able to recover it.
>
> After you register and login to this forum you will be able to fill out a detailed profile. For your security you should not post information here that can be used to identify you.
>
> Spam, flooding, advertisements, chain letters, pyramid schemes, and solicitations are forbidden on this forum.
>
> Note that it is impossible for the staff or the owners of this forum to confirm the true identity of users or monitor in realtime all messages posted, and as such we are not responsible for the content posted by those users. You remain solely responsible for the content of your posted messages.
>
> The forum software places a cookie, a text file containing bits of information (such as your username and password), in your browser's cache. This is ONLY used to keep you logged in/out. This website is not able to see your IP and [cannot] collect or send any other form of information to your computer except what you expressly upload. For your own security when browsing . . . Tor we also recommend that you turn off javascript and disable sending of the 'referer' header.

(Doc. 21-1 at 18-19.)

After the user accepts the above terms, Playpen requires the user to enter a username, password, and email address to complete the registration process. Only registered users are allowed to access the forum. *See id.* at 18 ("Warning! Only registered members are allowed to access the section. Please login below or 'register an account[.]'").

Once a user has logged into the Playpen using a registered account, he or she is presented with a index page which displays various forums and subforums including videos, photos, and webcams of : "Jailbait-Boy[,] Jailbait-Girl[,] Preteen-Boy[,] Preteen-Girl[,]" "Toddlers[,]" "Kinky Fetish[,]" "Bondage[,]" "Spanking[,]" "Girls H[ard]C[ore][,]" and "Boys H[ard]C[ore][.]" Some of these forums and subforums include thousands of posts. For example, there are 20,992 posts listed for "Girls HC." Gov't Ex. 2, *Michaud* – Ex. 5, at 00696-97. In addition to English, there are six foreign languages forums that enable Playpen users to communicate with other Playpen users in their own language.

According to Special Agent Alfin, although the posts on the Playpen website are not limited to child pornography, the "website in its entirety is dedicated to the advertisement and distribution of child pornography." Gov't Ex. 1, p. 28, lines 9-11. On this basis, he opined that there is probable cause that anyone accessing Playpen is doing so for unlawful purposes.

In 2014 and 2015, the FBI investigated Playpen and determined that it was operated from at least August 2014 until February 2015 on computer servers located in North Carolina. On February 19, 2015, the FBI identified and arrested the Playpen administrator in Naples, Florida. The following day, the FBI seized the computer server hosting the Playpen website and transferred the website to an FBI-controlled server located in the Eastern District of Virginia.

After gaining control of the Playpen server, because of the nature of the Tor network and Playpen's status as a hidden service, although the FBI could determine what each visitor to the Playpen website did, what posts he or she accessed, and which images of child pornography, if any, were downloaded, it had no ability to identify Playpen website users. *Id.* at 36. In order to complete this investigative step, the FBI sought judicial permission to operate the Playpen website from its server from February 20, 2015 until March 4, 2015 and sought to identify Playpen users through a "network investigative technique" ("NIT").

On February 20, 2015, pursuant to Fed. R. Crim. P. 41(c), the FBI presented to Magistrate Judge Buchanan a thirty-page search warrant application and affidavit which were reviewed by the U.S. Attorney's Office for the Eastern District of Virginia prior to their submission. With regard to its territorial limitations, the search warrant indicated that it was for persons or property located in the Eastern District of Virginia. It described the "[p]lace to be [s]earched" as "[t]he activating computers . . . of any user or administrator who logs into the TARGET WEBSITE by entering a username and password." (Doc. 21-1 at 3) (emphasis omitted). Based on the application presented, Magistrate Judge Buchanan found probable cause to authorize the FBI to deploy a NIT on Playpen from the government-controlled server in the Eastern District of Virginia (the "NIT warrant").

Although the NIT warrant authorized the FBI to deploy the NIT on any computer accessing Playpen, the FBI decided to narrow the warrant's scope by limiting the deployment of the NIT on only those "activating computers" that navigated to a Playpen post "that purported to advertise prepubescent female children engaged in penetrative sexual activity." Gov't Ex. 1, p. 45.[1] As Special Agent Alfin described it: "The user actively, they browse through the website and they open up that post. The NIT was deployed silently in the background without the user's knowledge." *Id.* at 46, lines 3-5.

Thereafter, the NIT and an "exploit"[2] obtained certain information from "activating computers" in a transmission generated by the NIT that took place in

[1] For certain moderators and administrators, the NIT was designed to deploy automatically once the Playpen website was accessed. Gov't Ex. 1, p. 46. There is no evidence this occurred in Defendant's case.

[2] Special Agent Alfin described the "exploit" as follows:

> [T]he exploit can be thought of an open window on the computer. And so the government, obviously we know about this open window and that's what we're able to send the NIT through. And so we use this exploit, the open window, and we send the NIT. . . . The NIT collects the information and sends it back to the government. The state of the window, it was open when we got there; it was open when we left. We did not have any impact or make any change to the window. . . . [The exploit] was not capable of making changes to the computer.

approximately .27 seconds. The NIT neither made changes to "activating computers," nor was capable of making them. Instead, it operated through:

> very simple computer commands that would . . . essentially . . . send the MAC address, send the operating system, send the username. It didn't go searching through the computer. The NIT was designed in such a manner that it could only collect and report the information identified. It did not have the capability or give the government the capability to rummage through files on the computer. We had no ability to look at what files they had on there, legal or illegal. It did not have the ability to search the content of the computer.

Id. at 84, lines 15-25.

After it was deployed, the NIT obtained and relayed the following information to the FBI-controlled Playpen server in the Eastern District of Virginia: (1) the "activating computer's" IP address, and the date and time the NIT determined the IP address; (2) a unique identifier generated by the NIT to distinguish between data from different computers; (3) the type, version, and architecture of the computer's operating system; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's host name; (6) the computer's active operating system user name; and (7) the computer's Media Access Control ("MAC") address.[3]

During the FBI's thirteen day period of operating the Playpen website, approximately 100,000 user accounts logged in and met the triggering condition for the NIT. Not all of those visits reflect individual users as it is common for Playpen users to create a new account with each login. The FBI's use of the NIT revealed over 1,300 IP addresses, including domestic and foreign users.

On February 25, 2015, the user "drscany" accessed Playpen and accessed the child pornography post containing the NIT. The NIT collected information from drscany's

Id. at 60-61. Although the NIT warrant did not use the term "exploit," "it did have a thorough breakdown of how the NIT was going to work and the information that was going to be collected." *Id.* at 62, lines 7-9.

[3] Computers connect to a network through a network adapter, most of which have a MAC address assigned by the adapter's manufacturer as a unique identifying number. Because a MAC address does not change and is unique, law enforcement can use it to identify whether communications sent or received at different times are associated with the same adapter.

computer and sent the information through the Internet to the FBI-controlled server in the Eastern District of Virginia. The NIT did not search the contents of drscany's computer files or allow the FBI or any other governmental entity to access drscany's computer at a later date.

Using the information obtained from the NIT, the FBI determined that drscany's IP addressed was operated by Comcast and was linked to an account located at 60 Rocky Road in Richmond, Vermont. On December 21, 2015, Magistrate Judge John Conroy authorized a search warrant for 60 Rocky Road in Richmond, Vermont, which was executed on December 22, 2015, and resulted in evidence incriminating Defendant.

II. Legal Analysis and Conclusions.

A. Standard of Review.

In a suppression hearing, "[i]t is well established that the burden of production and persuasion generally rest upon the movant[.]" *United States v. Arboleda*, 633 F.2d 985, 989 (2d Cir. 1980) (internal quotation marks omitted). "[T]he controlling burden of proof at suppression hearings should impose no greater burden than proof by a preponderance of the evidence." *United States v. Matlock*, 415 U.S. 164, 177 n.14 (1974).

Where, as here, there is a challenge to a search warrant, the court begins with the presumption that the warrant is valid. *See United States v. Rosa*, 11 F.3d 315, 326 (2d Cir. 1993) ("A search warrant issued by a neutral and detached magistrate is entitled to substantial deference, and doubts should be resolved in favor of upholding the warrant") (internal quotation marks omitted); *United States v. Demosthene*, 326 F. Supp. 2d 531, 536 (S.D.N.Y. 2004) ("A search warrant is presumptively valid").

B. Whether the NIT Warrant was Void Ab Initio.

Defendant contends that the NIT warrant was void ab initio because it authorized a search of property outside Magistrate Judge Buchanan's jurisdiction. He argues that suppression on that basis alone is required. The problem with this argument is twofold.

First, even if a magistrate judge in the Eastern District of Virginia does not have jurisdiction to issue a search warrant for "property"[4] located in Vermont, it is beyond dispute that Magistrate Judge Buchanan had jurisdiction to authorize a search of "property" located within her jurisdiction. *See United States v. Anzalone*, 2016 WL 5339723, at *11 (D. Mass. Sept. 22, 2016) ("Even if the magistrate judge in the Eastern District of Virginia lacked the authority to issue a warrant that allowed the FBI to deploy the NIT outside of that district, the magistrate judge did have authority to issue a warrant in which the NIT deployed in that district. The warrant was not void at its issuance."). It is further undisputed that the NIT was deployed in the Eastern District of Virginia and obtained IP addresses of computers there. *See, e.g.*, *United States v. Matish*, 193 F. Supp. 3d 585, 612 (E.D. Va. 2016) (denying motion to suppress where NIT warrant obtained IP addresses and other information from computers in the Eastern District of Virginia); *United States v. Eure*, 2016 WL 4059663, at *1 (E.D. Va. July 28, 2016) (rejecting suppression where magistrate judge had jurisdiction to issue the NIT warrant where government "operated [the Playpen website] from a government facility in the Eastern District of Virginia"). Accordingly, at best, the NIT warrant was only partially invalid and was thus not void ab initio. *See Conlin v. Mortg. Elec. Registration Sys., Inc.*, 714 F.3d 355, 361 n.6 (6th Cir. 2013) ("Void ab initio is defined as null from the beginning") (internal quotation marks and italics omitted); Black's Law Dictionary (10th ed. 2014) (defining "void ab initio" as "[n]ull from the beginning, as from the first moment when a contract is entered into.").

Second, to the extent Defendant claims that Magistrate Judge Buchanan was required to limit the NIT warrant's reach to the Eastern District of Virginia, he does not explain how this could be achieved. The magistrate judge did not *choose* the computers

[4] Some courts have concluded that the NIT warrant authorized a "search" of a "computer" located in another jurisdiction. *See, e.g.*, *United States v. Anzalone*, 2016 WL 5339723, at *6 (D. Mass. Sept. 22, 2016) (cautioning against a narrow scope of inquiry in deciding whether the NIT warrant was authorized and "asking 'whether the IP address should be the focus of this analysis or whether Defendant's expectation of privacy in his computer is the proper subject of this analysis.'") (quoting *United States v. Adams*, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016)).

on which the NIT was deployed, nor could she reasonably do so. Instead, the NIT was deployed on the "activating computers" of individuals located both within and outside the Eastern District of Virginia because those individuals reached out to the Playpen website and accessed the NIT embedded in a child pornography post. It was thus Playpen users who reached out to the Eastern District of Virginia, not the other way around. *See United States v. Darby*, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016) ("Users of Playpen digitally touched down in the Eastern District of Virginia when they logged into the site."). Although Magistrate Judge Buchanan could have required the FBI to reject evidence from any IP addresses not located in the Eastern District of Virginia, this would not have prevented the NIT from allegedly searching for and seizing those IP addresses in the first instance.

Because the NIT strayed beyond the confines of the Eastern District of Virginia as a result of the technology used and the voluntary actions of Playpen users, and not because of Magistrate Judge Buchanan's willful disregard of the territorial limits of her jurisdiction, there is no basis for finding the NIT warrant was void ab initio. *United States v. Krueger*, 809 F.3d 1109, 1115 (10th Cir. 2015), on which Defendant relies, does not require a different result. There, the government conceded a violation of Fed. R. Crim. P. 41 when a magistrate judge issued a search warrant for property located in another district. The only issue was whether this Rule 41 violation caused the defendant prejudice. The Tenth Circuit cabined its decision to the unremarkable conclusion that the defendant proffered sufficient evidence of prejudice because, but for the Rule 41 violation, the search warrant would not have issued. The Tenth Circuit "expressly [did] not address the propriety of suppression when, at the time of issuance, it is genuinely unclear whether the federal magistrate judge has authority to issue an outside-of-district warrant." *Krueger*, 809 F.3d at 1113 n.4. The Tenth Circuit also did not determine whether the Rule 41 violation was of constitutional magnitude. However, it noted that: "Over the years, we have addressed many other provisions of Rule 41, never concluding that the alleged Rule 41 violation(s) at issue justified suppression." *Id.* at 1115 n.7 (collecting cases).

Reliance on *Krueger* for the proposition that the NIT warrant is void ab initio ignores the careful limits of that decision. Even as persuasive authority, *Krueger* does not dictate the outcome where, as here, there is a genuine dispute, not only among the litigants, but among the courts, regarding whether a Rule 41 violation occurred.[5]

C. Whether Fed. R. Crim. P. 41 Authorized the NIT Warrant.

At the time of the NIT warrant's issuance, Rule 41 stated in relevant part as follows:

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
>
> > (1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
> >
> > (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
> >
> > . . .
> >
> > (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both[.]

Fed. R. Crim. P. 41(b)(1),(2), & (4) (emphasis omitted).

Effective December 1, 2016, Rule 41 was amended to specifically authorize NIT warrants:

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote

[5] [C]ourts have generally reached one of three results: either (1) the NIT warrant was unlawfully issued and suppression is required; (2) the NIT warrant was unlawfully issued, but suppression is not the appropriate remedy; or (3) the NIT warrant was lawfully issued, and there are no legal violations that require suppression.

United States v. Dzwonczyk, 2016 WL 7428390, at *6 (D. Neb. Dec. 23, 2016).

> access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> > (A) the district where the media or information is located has been concealed through technological means; or
> >
> > (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Fed. R. Crim. P. 41(b)(6) (emphasis omitted).

Defendant argues that "the failure of the NIT warrant to comply with Rule 41(b) is highlighted by the . . . amendments to Rule 41(b), which . . . authorize searches such as that accomplished via the NIT" and that "[t]he fact that a new subsection [was] added to Rule 41(b) to permit the issuance [of] warrants such as the NIT warrant at issue here, strongly suggests that Rule 41(b) did not authorize such warrants in February 2015 when the NIT warrant was issued." (Doc. 21 at 9-10.) Although this argument has some merit, the amendments to Rule 41 do not purport to expand a magistrate judge's jurisdiction or authorize warrants that were previously unlawful. Instead, as the Advisory Committee Notes reveal, the amendments were intended only to reflect advances in technology that render a "territorial" or "venue" restriction on certain types of search warrants nonsensical:

> Rule 41's territorial venue provisions—which generally limit searches to locations within a district—create special difficulties for the [g]overnment when it is investigating crimes involving electronic information. The proposal speaks to two increasingly common situations affected by the territorial restriction, each involving remote access searches, in which the government seeks to obtain access to electronic information or an electronic storage device by sending surveillance software over the Internet.
>
> In the first situation, the warrant sufficiently describes the computer to be searched, but the district within which the computer is located is unknown. This situation is occurring with increasing frequency because persons who commit crimes using the Internet are using sophisticated anonymizing technologies[] . . . [such as] proxy services designed to hide their true IP addresses. Proxy services function as intermediaries for Internet communications: when one communicates through an anonymizing proxy service, the communication passes through the proxy, and the recipient of the communication receives the proxy's IP address, not the originator's true

> IP address. Accordingly, agents are unable to identify the physical location and judicial district of the originating computer. . . . The second situation involves the use of multiple computers in many districts simultaneously as part of complex criminal schemes.

Report of the Advisory Committee on Criminal Rules to the Committee on Rules of Practice and Procedure (May 6, 2015).

It would produce an anomalous result if a search warrant that was invalid and without jurisdiction on November 30, 2016 became valid and within a magistrate judge's jurisdiction on December 1, 2016 simply because the amendments to Rule 41 took effect. Certainly the amendments to Rule 41 do not purport to effect that dramatic change. Moreover, although the NIT warrant was not clearly authorized by the plain language of Rule 41, its issuance was nonetheless consistent with applicable law. The Supreme Court has long held that Fed. R. Crim. P. 41 "is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause." *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 169 (1977); *see also* 18 U.S.C. § 3103a(a) (authorizing a warrant to "be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States"). It is thus questionable whether Defendant can prove that a Rule 41 violation took place.

The government fares no better in urging the court to find the NIT warrant authorizes a "tracking device" under Rule 41(b)(4) because "[t]he NIT in this case functioned in a similar manner in the context of the Internet." (Doc. 22 at 5.) A "tracking device" under Rule 41 is defined by 18 U.S.C. § 3117(b) as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Section 3117(a) provides that "[i]f a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction *if the device is installed in that jurisdiction*." *Id.* at § 3117(a) (emphasis supplied).

In this case, the NIT did not "track" the movement of Defendant or his computer and it did not "track" the movement of files or computer code. *See United States v. Croghan*, 2016 WL 4992105, at *4 (S.D. Iowa Sept. 19, 2016) ("The NIT here at issue, however, clearly did not 'track' the 'movement of a person or object.' Indeed, it did not 'track' the 'movement' of anything; rather, it caused computer code to be installed on the activating user's computer, which then caused such computer to relay specific information to the government-controlled computers in Virginia.").

In addition, the NIT was not "installed" in the District of Vermont. If it was "installed" anywhere, it was "installed" in the Eastern District of Virginia when Defendant allegedly electronically visited the Playpen website, accessed the NIT-containing post, and returned with computer code that compelled his computer to relay certain information to a FBI-controlled server. Rule 41(b)'s tracking device provision as applied to the NIT warrant therefore "stretches the rule too far." *United States v. Eldred*, Case No. 5:16-cr-89, Doc. 25 at 10 (D. Vt. Feb. 17, 2017) (quoting *United States v. Michaud*, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016) (concluding that reliance on Rule 41(b)(4) "stretches the rule too far" because "[i]f the 'installation' occurred on the government-controlled computer, . . . applying the tracking device exception breaks down, because [defendant] never controlled the government-controlled computer" and "[i]f the installation occurred on [defendant's] computer, applying the tracking device exception again fails, because [defendant's] computer was never physically located within the Eastern District of Virginia")).[6]

Based on the foregoing, the court assumes without deciding that a Rule 41 violation occurred and proceeds to determine whether suppression is warranted. In the

[6] Most courts have reached a similar conclusion. *See, e.g.*, *United States v. Werdene*, 188 F. Supp. 3d 431, 442 (E.D. Pa. 2016) (holding that Rule 41(b)(4) did not authorize the NIT warrant because the computer targeted was at all times outside of the Eastern District of Virginia); *United States v. Henderson*, 2016 WL 4549108, at *4 (N.D. Cal. Sept. 1, 2016) (finding no authority under Rule 41(b)(4) in part because "the NIT was installed outside of the district, at the location of the activating computers, not within the district as required by Rule 41(b)(4)"); *United States v. Allain*, 2016 WL 5660452, at *11 (D. Mass. Sept. 29, 2016) ("Even if the [c]ourt agreed with the tracking device analogy, the NIT [w]arrant would still not be permitted under Rule 41(b)(4), since the NIT was not installed in the Eastern District of Virginia. . . . The NIT was downloaded from the Playpen server . . . and placed onto the 'activating' computers . . . . Given that the 'activating' computers never entered the Eastern District of Virginia, it stretches the rule too far to say that the installation occurred within the Eastern District of Virginia.").

Second Circuit, it is well-settled that, provided they are not of "constitutional magnitude":

> violations of Rule 41 alone should not lead to exclusion [of evidence] unless (1) there was "prejudice" in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule.

United States v. Burke, 517 F.2d 377, 386-87 (2d Cir. 1975) (footnotes omitted). The court therefore turns to the whether the NIT warrant violated the Fourth Amendment.

D. Whether the NIT Warrant Violated the Fourth Amendment.

"The Fourth Amendment protects the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]'" *United States v. Stokes*, 733 F.3d 438, 443 (2d Cir. 2013) (quoting *Kentucky v. King*, 563 U.S. 452, 459 (2011)). "As the text makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness." *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (internal quotation marks omitted).

Fourth Amendment rights "are personal, and may be enforced only by persons whose *own* protection under the Amendment has been violated." *United States v. Fields*, 113 F.3d 313, 320 (2d Cir. 1997); *see also Katz v. United States*, 389 U.S. 347, 351 (1967) (explaining that "the Fourth Amendment protects people, not places"). For this reason, a "defendant seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment must show that he had a 'legitimate expectation of privacy' in the place searched." *United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 (1978) (defining "the scope of the interest protected by the Fourth Amendment" as "whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place")). "This inquiry involves two distinct questions: first, whether the individual had a subjective expectation of privacy; and second, whether that expectation of privacy is one that society accepts as reasonable." *Id.*

Although the Second Circuit has held that "[i]ndividuals generally possess a reasonable expectation of privacy in their home computers[,]" *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004), and has concluded that certain office computers offer this same expectation of privacy, *see Leventhal v. Knapek*, 266 F.3d 64, 73-74 (2d Cir. 2001) (finding defendant had a reasonable expectation of privacy in the contents of his computer located in a private office to which no one else had access), it has never been called upon to consider whether there is a reasonable expectation of privacy in the circumstances presented here. Courts outside the Second Circuit have reached divergent conclusions regarding whether the NIT warrant authorized a "search" of the "contents" of a computer, or whether it retrieved only publicly available information in which no reasonable expectation of privacy exists.[7]

[7] *Compare United States v. Darby*, 190 F. Supp. 3d 520, 530 (E.D. Va. 2016) ("[I]f an individual has a reasonable expectation of privacy in the contents of his or her personal computer, as he or she does, and the deployment of the NIT invades that privacy, then the NIT is a search. The NIT in this case caused [d]efendant's computer to download certain code without the authorization or knowledge of [d]efendant. The 'contents' of a computer are nothing but its code. In placing code on [d]efendant's computer, the government literally—one writes code—invaded the contents of the computer. . . . [I]t is irrelevant that [d]efendant might not have a reasonable expectation of privacy in some of the information searched and seized by the government. The government's deployment of the NIT was a Fourth Amendment search."), *and Allain*, 2016 WL 5660452, at *7 n.5 ("The [c]ourt . . . finds that the FBI did need to obtain a warrant in order to use the NIT. The FBI's search not only implicated defendant's privacy interest in his IP address, but also in his computer. Although an IP address may be obtained from a third party provider and therefore arguably carries with it a lower expectation of privacy, in this case, the FBI needed to install a program that searched through [defendant's] computer to get the IP address. Regardless of whether and to what extent [defendant] had a privacy interest in his IP address, he most certainly had a reasonable expectation of privacy in the contents of his computer."), *with United States v. Acevedo-Lemus*, 2016 WL 4208436, at *3 (C.D. Cal. Aug. 8, 2016) ("The [c]ourt concludes that the FBI's acquisition of the key piece of information here—[d]efendant's IP address—was not a search under the meaning of the Fourth Amendment, and therefore did not require a warrant"); *United States v. Matish*, 193 F. Supp. 3d 585, 615 (E.D. Va. 2016) ("Defendant possessed no reasonable expectation of privacy in his computer's IP address, so the [g]overnment's acquisition of the IP address did not represent a prohibited Fourth Amendment search."); *Werdene*, 188 F. Supp. 3d at 446 ("Since [defendant] did not have a reasonable expectation of privacy in his IP address, the NIT cannot be considered a 'search' within the meaning of the Fourth Amendment"); *United States v. Lough*, 2016 WL 6834003, at *4 (N.D. W. Va. Nov. 18, 2016) (noting that whatever expectation of privacy defendant may generally have in the contents of his personal computer, "the FBI's use of the NIT to discover [defendant's] IP address was not a search of the contents of that computer.").

From a technological standpoint, the NIT warrant did not authorize a search of the contents of Defendant's computer. *See United States v. Acevedo-Lemus*, 2016 WL 4208436, at *6 (C.D. Cal. Aug. 8, 2016) (observing that "the NIT obtained *very* limited information from [d]efendant's computer" and "did not, for example, search for files containing child pornography or otherwise inspect the computer's contents" but rather its "crucial operation" was to obtain the defendant's IP address, which is information that is "normally public and often disclosed to third parties"). It also did not alter Defendant's computer, deposit code on it, or retrieve any information in which courts have recognized a reasonable expectation of privacy.

Any "search" occurred only after Defendant voluntarily connected his computer to the Internet, downloaded the browser and Tor software, registered a Playpen account, and accessed the NIT-containing child pornography post on the Playpen website. In engaging in these voluntary actions, a reasonable computer user may be deemed to have understood that he or she was potentially conveying certain information to third party computers and servers in order to allow the transfer of information to take place. *See United States v. Dzwonczyk*, 2016 WL 7428390, at *9 (D. Neb. Dec. 23, 2016) (finding no reasonable expectation of privacy in IP address and noting that "an individual 'necessarily shares the IP address assigned to his computer to and from third parties[.]'"). Indeed, Playpen warned its users not to use their real email addresses and cautioned that "[t]he forum software places a cookie, a text file containing bits of information (such as your username and password), in your browser's cache." (Doc. 21-1 at 19, ¶ 13.) It further advised: "[f]or your own security, you should not post information here that can be used to identify you" and "[f]or your own security[,] when browsing . . . Tor we also recom[m]end that you turn off javascript and disable sending of the 'referer' header." *Id.* (internal quotation marks omitted). Against this backdrop, any expectation by a Playpen user that his or her identity could not and would not be revealed while accessing child pornography on a publicly available website is not one society would deem reasonable. *See Hamilton*, 538 F.3d at 167 (holding no Fourth Amendment violation occurs if the "expectation of privacy is [not] one that society accepts as reasonable"). The court therefore concludes that the NIT warrant did not violate the Fourth Amendment and any Rule 41 violation was not of constitutional magnitude.

The court assumes that Defendant will be able to show prejudice as, without the alleged Rule 41 violation, his identity would not have been discovered. *See United States v. Adams*, 2016 WL 4212079, at *8 (M.D. Fla. Aug. 10, 2016) ("The application in support of the NIT warrant makes it abundantly clear that law enforcement had no realistic chance of identifying the IP address associated with [d]efendant's computer without the NIT."). The court therefore examines whether any Rule 41 violation was intentional and deliberate and concludes that it was not.

At the time the NIT warrant was issued, only one magistrate judge in the country had concluded that Fed. R. Crim. P. 41 did not authorize a NIT search warrant. *See In re Warrant to Search a Target Comput. at Premises Unknown*, 958 F. Supp. 2d 753, 758 (S.D. Tex. 2013). This precedent was not controlling in the Eastern District of Virginia and government officials were not required to refrain from seeking NIT warrants while they sought amendments to Rule 41.

In seeking the NIT warrant, the government disclosed to Magistrate Judge Buchanan that the NIT warrant "involved sophisticated and novel technology—used both by the operators and users of Playpen as well as the federal investigators—and the FBI made a reasonable attempt to structure a search warrant that complied with rules that have not evolved as quickly as the technology." *United States v. Allain*, 2016 WL 5660452, at *12 (D. Mass. Sept. 29, 2016). As a result:

> [t]he FBI agents in this case did the right thing. They gathered evidence over an extended period and filed a detailed affidavit with a federal magistrate in support of their search warrant application. They filed the warrant application in the federal district that had the closest connection to the search to be executed. The information gathered by the warrant was limited: primarily the IP addresses of those that accessed Playpen and additional information that would aid in identifying what computer accessed the site and what individual used that computer. . . . [T]he officers in charge of this investigation are not at all culpable. . . . [T]here is no evidence that any failure by the FBI to understand the intricacies of the jurisdiction of federal magistrates was deliberate.

Darby, 190 F. Supp. 3d at 538. Any violation of Rule 41 was therefore neither flagrant nor deliberate.

On balance, although Defendant can show prejudice, the court concludes suppression is not warranted because: (1) the Eastern District of Virginia had the greatest connection to the Playpen server; (2) the magistrate judge could not control or limit where the NIT was deployed; (3) users of "activating computers" played an essential role in determining where the NIT was deployed; (4) probable cause for the NIT warrant is not challenged; (5) law enforcement sought and obtained judicial authorization for the NIT and operation of the Playpen website; and (6) Rule 41 as it existed at the time did "not directly address the kind of situation that the NIT [w]arrant was authorized to investigate, namely, where criminal suspects['] geographical whereabouts are unknown, perhaps by design, but the criminal suspects had made contact via technology with the FBI in a known location." *Michaud*, 2016 WL 337263, at *6. No different outcome is warranted if the court assumes *arguendo* that a Fourth Amendment violation took place.

Under *United States v. Leon*, 468 U.S. 897, 922 (1984),[8] the exclusionary rule is a "deterrent sanction" created by the Supreme Court to "bar[] the prosecution from introducing evidence obtained by way of a Fourth Amendment violation." *Davis v. United States*, 564 U.S. 229, 231-32 (2011). The Supreme Court has cautioned that "exclusion '[should be] our last resort, not our first impulse[.]'" *Herring v. United States*, 555 U.S. 135, 140 (2009). The rule deters "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id.* at 144. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.*

In this case, the government obtained the NIT warrant only after truthfully advising Magistrate Judge Buchanan how the NIT would work, what information it would retrieve, and from where it would retrieve it. Thereafter, the government relied on

[8] Defendant's argument that the exclusionary rule does not apply is premised upon his erroneous assumption that the NIT warrant was void ab initio.

the NIT warrant in good faith and, indeed, narrowed the scope of the warrant so that the NIT generally only deployed when a user reached out to the Playpen website and accessed what appeared to be a child pornography post. Suppression of the evidence obtained through the NIT warrant would not deter future police misconduct—the sole purpose of the exclusionary rule. *See United States v. Broy*, 209 F. Supp. 3d 1045, 1058-59 (C.D. Ill. 2016) (observing that "the only benefit to suppression in this case would be ensuring magistrate judges are more careful about issuing NIT warrants in the future" and that "the exclusionary rule is designed to control the conduct of *law enforcement*, not the conduct of federal judges"); *United States v. Werdene*, 188 F. Supp. 3d 431, 452 (E.D. Pa. 2016) (stating that "to the extent a mistake was made in this case, it was not made by the agents in 'reckless . . . disregard for Fourth Amendment rights[]'" but instead "made by the magistrate when she mistakenly issued a warrant outside her jurisdiction"); *Michaud*, 2016 WL 337263, at *7 ("Because reliance on the NIT [w]arrant was objectively reasonable, the officers executing the warrant acted in good faith, and suppression is unwarranted.").

Because there was good faith reliance by law enforcement on a search warrant supported by probable cause, the court concludes that the exclusionary rule applies and that any violation of the Fourth Amendment that took place does not warrant the "last resort" of suppression. *See Herring*, 555 U.S. at 140.

CONCLUSION

For the foregoing reasons, the court hereby DENIES Defendant's motion to suppress evidence and statements. (Doc. 21.)

SO ORDERED.

Dated at Burlington, in the District of Vermont, this 26th day of April, 2017.

Christina Reiss, Chief Judge
United States District Court